(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年5 月30 日 (30.05.2002)

PCT

(10) 国際公開番号
WO 02/42890 A1

(51) 国際特許分類[7]: G06F 1/00, 15/00, H04L 9/32

(21) 国際出願番号: PCT/JP00/08256

(22) 国際出願日: 2000 年11 月22 日 (22.11.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 岩佐直樹 (IWASA, Naoki) [JP/JP]. 佐久間春久 (SAKUMA, Haruhisa) [JP/JP]. 川崎 誠 (KAWASAKI, Makoto) [JP/JP]. 原田義久 (HARADA, Yoshihisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 石田 敬, 外 (ISHIDA, Takashi et al.); 〒105-8423 東京都港区虎ノ門三丁目5番1号 虎ノ門37森ビル 青和特許法律事務所 Tokyo (JP).

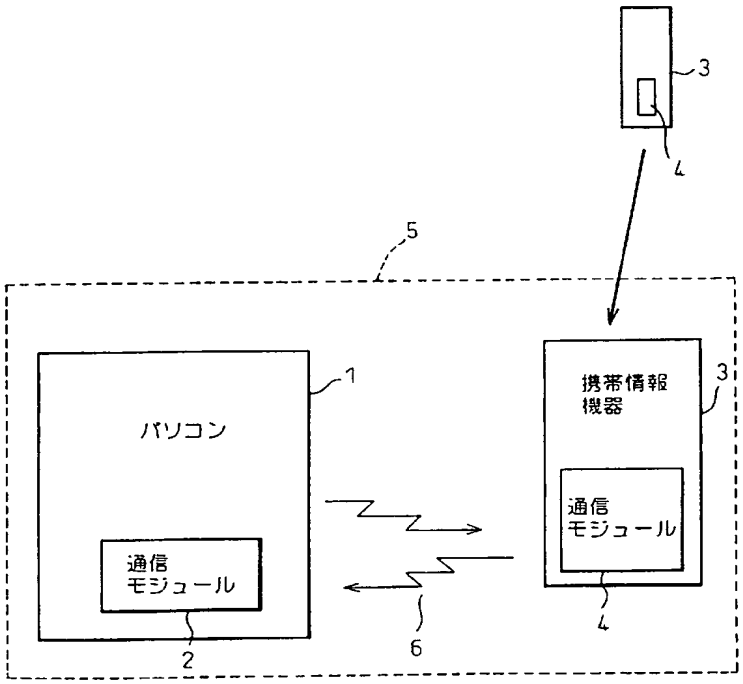
(81) 指定国 (国内): JP, US.

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: SECURITY SYSTEM FOR INFORMATION PROCESSOR

(54) 発明の名称: 情報処理装置のセキュリティシステム



1...PERSONAL COMPUTER
2...COMMUNICATION MODULE
3...PORTABLE INFORMATION TERMINAL
4...COMMUNICATION MODULE

(57) Abstract: An information processor includes a first communication module for wireless data communication. A portable information terminal includes a second communication module capable of establishing a wireless communication link with the first communication module. The information processor is adapted to indicate a password input screen only if a communication link is established between the first and second communication modules. The first and second communication modules are Bluetooth-compatible. The information processor will not start up the operating system unless any registered portable information terminal is located near the information processor and a correct password is entered. As a result, an information processor security system is provided with a double check function.

WO 02/42890 A1

[続葉有]

(57) 要約:

無線によるデータ通信が可能な第１の通信モジュールを備えた情報処理装置と、前記第１の通信モジュールと無線通信リンクを形成可能な第２の通信モジュールを備えた携帯情報機器とを備え、前記情報処理装置を、前記第１および前記第２の通信モジュール間で通信リンクが形成された場合のみパスワード入力画面に移行するように設定する。この第１、第２の通信モジュールはブルートゥース対応の通信モジュールである。この装置では、予め登録された携帯情報機器が情報処理装置の近くにあり、かつ正常なパスワードが入力されない限り、情報処理装置はＯＳを起動しない。これにより、２重のチェック機構を備えた情報処理装置のセキュリティシステムを提供することができる。

明 細 書

情報処理装置のセキュリティシステム

技術分野

本発明は、パーソナルコンピュータ（以下、パソコンと言う）等の情報処理装置の正規の使用者(以下、ユーザーと言う）を特定するための強化されたセキュリティシステムに関し、特に、そのために特別のハードウエア及びそれを起動するアプリケーションを追加することなく、汎用の機器によって簡単に構成することができるセキュリティシステムに関する。

従来技術

ハードディスクがますます小型で大容量化しかつ価格が低下するにしたがって、パソコン内に重要な書類を電子化して保存する傾向が強くなっている。これに伴って、パソコンを如何に安全に管理するかが重要な問題となっている。

現在一般的に使用されているパソコンのセキュリティ装置では、ＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）と呼ばれる基本プログラムによりパスワード設定を行い、キーボードからユーザーがパスワードを正しく入力することによって始めてＯＳを起動させている。即ち、ＢＩＯＳＢＩＯＳに予め登録されたパスワードによってそのパソコンの使用者を特定する設計となっている。

しかしながら、パスワードとして個人特有の情報、例えば生年月日、電話番号、愛称等を選択する傾向が強く、パスワードを他人が知ることは比較的容易である。また一旦パスワードが他人に知られ

ると、そのパソコンは他人に容易に使用される。

パスワードに加えてさらにセキュリティを強化するために、指紋認証装置の利用やあるいはパソコンに加速度センサを取り付けてパソコンの移動を検出するとシステムをシャットダウンしてしまうように設計されたものも提案されている。しかしながらこれらの装置はその実現のために特別なハードウエアおよびアプリケーションソフトの開発が必要であり、さらにユーザーがパスワード、指紋認証装置等によるセキュリティチェックをクリアしてパソコンを使用状態に設定した後席を離れた場合等では、他人によってパソコンが容易に不正使用される。

この欠点を解決するために、例えば特開平９－１５３０１６号公報に記載の発明「パソコン使用者特定システムおよびパソコン使用者特定方法」では、特定のパソコンの使用を許可された者のＩＤ情報をワイヤレスＩＣカードに記憶しておき、これをユーザーが携帯し、パソコンとの間で無線によるＩＤ情報の送受信を行ってユーザーを確認する技術を提案している。

この発明では、ＩＤ情報がパソコンに入力されている限りにおいてパソコンの使用を許可している。従って、ユーザーがカードとパソコンとの間の無線通信エリアを離れると、ＩＣカードからのＩＤ情報の送信が停止され、パソコンはシステムを自動的にシャットダウンする。これによってユーザーがパソコンを使用状態にして席を離れた場合の他人によるパソコンの不正使用を防止している。

しかしながらこの方法および装置では、ワイヤレスＩＣカードおよびパソコンの近くに読み取り器等の特別なハードウエアを配置する必要があるため装置が複雑と成ると共に、さらにワイヤレスＩＣカードを盗用されてしまえば、それ以上他人による不正使用を防ぐ手段はない。

‘０１６号公報に記載の発明と同様の趣旨で、携帯電話、ＩＤカードを使用してワイヤレスでＩＤ情報を送信し、ワークステーションへ簡単にログインする技術が、特開平８－３０７４１２号公報に記載の発明「自動ログイン方法及びシステム」において提案されている。しかしながら、この場合も携帯電話、ＩＤカード等が盗用された場合のセキュリティチェックシステムについては何ら考察されておらず、従って何らの対策も設定されていない。

発明の要約

本発明は、情報処理装置における従来のセキュリティシステムの上記欠点に鑑みてなされたものであり、特別なハードウエアおよびアプリケーションソフトを開発することなく、しかも簡単な装置でセキュリティを強化することが可能な、情報処理装置のセキュリティシステムを提供することを目的とする。

さらに、パスワード入力済みの状態で使用者が情報処理装置から離れた場合でも、自動的にセキュリティシステムを作動させて他人による不正使用を防止することが可能な、情報処理装置のセキュリティシステムを提供することを目的とするものである。

上記目的を達成するために、本発明では、無線によるデータ通信が可能な第１の通信モジュールを備えた情報処理装置と、前記第１の通信モジュールと無線通信リンクを形成可能な第２の通信モジュールを備えた携帯情報機器とを備え、前記情報処理装置は、前記第１および前記第２の通信モジュール間で通信リンクが形成された場合のみパスワード入力画面に移行するように設定されている、情報処理装置のセキュリティシステムを提供する。

この装置では、予め登録された認証情報を有する携帯情報機器が情報処理装置の近くにあり、かつ予め登録されたパスワードがユー

ザーによって入力されない限り、情報処理装置はＯＳを起動しない。これによって、２重のセキュリティチェック機構が容易に構成される。

また、前記情報処理装置は前記携帯情報機器から予め登録されたパスワードの入力を受信した場合のみＯＳを起動するように構成されている。これによってさらに密接に情報処理装置と特定の携帯情報機器を結びつける事が可能となり、さらにセキュリティが強化される。

さらに前記第１、第２の通信モジュールはブルートゥース対応の通信モジュールで構成する。これによって、セキュリティチェックのための特別なハードウエアおよびアプリケーションソフトの構築を必要とせず、従来の情報処理装置と携帯情報機器にブルートゥース対応の通信モジュールを装着することによって、本発明の装置を容易に構成する事ができる。またブルートゥース機器の場合は、複数の機器との間でピコネットを形成することができるので、複数の携帯情報機器にそれぞれ異なるパスワードを対応させることによって、１台の情報処理装置を複数のユーザーで互いのセキュリティを保持しながら共用することが容易である。

またさらに、前記情報処理装置はＯＳの起動中において、前記第１および第２の通信モジュール間で通信リンクが切れたことを認識して入力デバイスをロック状態に移行させる構成をとっている。またさらに、リジュームボタンが操作されると、前記第１と第２の通信モジュール間で通信リンクが確立されている場合のみパスワード入力画面に移行し、予め登録されたパスワードの入力によって、上記入力デバイスのロック状態を解除する構成とされている。

これらの構成により、正規のユーザーが情報処理装置を使用状態にして不用意に席を離れた場合であっても、他人による情報処理装

置の不正使用を防止する事ができる。

図面の簡単な説明

図１は、本発明の１実施形態にかかる情報処理装置のセキュリティシステムを示すブロック図である。

図２は、図１に示すセキュリティシステムの動作を説明するためのフローチャートである。

図３は、セキュリティメニューセットアップ用の画面を示す。

図４（ａ）は、ユーザー用パスワード設定画面を示す図である。

図４（ｂ）は、ユーザー用パスワード変更画面を示す図である。

図５は、情報処理装置の使用中における図１のセキュリティシステムの動作を説明するためのフローチャートである。

図６は、情報処理装置のスリープ状態からの復帰時の、図１に示すセキュリティシステムの動作を説明するためのフローチャートである。

図７は、図１に示す情報処理装置の概略構成を示すブロック図である。

実施例

本発明の１実施形態として、情報処理装置にパソコンを用いた場合のセキュリティシステムを図１に示す。このシステムは、データ通信が可能な専用無線通信装置とアンテナからなる通信モジュール２を組み込んだパソコン１と、同様の専用無線通信装置とアンテナからなる通信モジュール４を組み込んだ携帯情報機器３とで構成される。この通信モジュール２および４は、１実施形態ではブルートゥース対応の専用通信チップであり、また携帯情報機器３は携帯電話あるいはＰＤＡ(Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉ

ｓｔａｎｃｅ）である。

以下、通信モジュール２，４がブルートゥース対応の通信モジュールである実施形態について、本発明を詳細に説明する。ブルートゥース対応の通信モジュール２，４は、短い信号、即ち認証情報を出し合って相互を確認しあっており、近距離に配置された複数の機器が無線リンクを形成することが可能である。通信距離は、室内程度あるいは１家屋内程度の選択が可能である。

ブルートゥース対応の通信モジュール２，４は以下のステップを踏んで互いを認識している。まず、１）パソコン１および携帯情報機器３の電源がオフの場合であっても、それぞれの通信モジュール２，４の電源がオンの場合は、互いに常に微弱な電波を一定間隔で送信し、周辺にブルートゥース対応の機器があるかどうかを探している。携帯情報機器３がパソコンの設定された通信可能範囲５内にない場合は、パソコン１側の通信モジュール２と携帯情報機器３側の通信モジュール４間に通信リンクは形成されない。この場合、通信モジュール２，４はＳｔａｎｄｂｙ（スタンバイ）モードにある。

次に、２）携帯情報機器３が通信可能範囲５内に入ってくると、パソコン１内の通信モジュール２は周辺にブルートゥース対応のモジュールがあることを認識し、サービスの獲得に乗り出す。これによって、３）パソコン１と携帯情報機器３間で認識情報を交換し合いピコネット６を形成する。このとき、パソコン１はマスタ、携帯情報機器３はスレーブとなる。この状態はＨｏｌｄ（ホールド）モードである。

以上のようにしてパソコン１と携帯情報機器３間に通信リンクが確立されるが、これらの処理はブルートゥース通信モジュール内のファームウエアで行われるので、パソコンおよび携帯情報機器の電

源のオン、オフに拘わらず実行される。

パソコン１側の通信モジュール２と携帯情報機器３側の通信モジュール４が通信リンクを確立した状態で、パソコン１の電源が既にオンとなっており、ＢＩＯＳ上のブルートゥースウェイクアップ設定が有効であれば、ブルートゥース通信モジュールからウェイクアップ要求が発生し、パソコン１は自動的に起動される。

一方、リンクが確立した時点でパソコン１の電源がオフであり、ＢＩＯＳ上のブルートゥースウェイクアップ設定が無効であれば、各通信モジュールはＨｏｌｄモードを維持する。この場合、パソコン１を起動するためにはユーザーが電源スイッチをオンとする必要がある。

図２は、ユーザーがパソコン１の電源をオンとした場合の、ＢＩＯＳ上でのセキュリティチェックの手順を示すフローチャートである。ＢＩＯＳ上でのセキュリティ情報は起動パスワード等を保存する不揮発性メモリ中のセキュリティ情報領域に予め保存されており、この領域は一般利用者（ユーザー）による変更が禁止されている。

まず、ユーザーによってパソコン１の電源が投入される（ステップＳ１）と、パソコン１の基本プログラムであるＢＩＯＳが作動して、セキュリティチェック用に予め登録された認識ＩＤを持つ携帯情報機器が近くにあるか否かを判断する（ステップＳ２）。

携帯情報機器３が通信モジュール２の通信可能範囲の外にある場合には、図１の説明の部分で述べたように、携帯情報機器３の通信モジュール４との間で無線リンクが形成されないので、ステップＳ２ではＮｏと判断され、ＢＩＯＳは次のステップに進まない。

一方、携帯情報機器３が通信可能範囲内に入ってきた場合、即ちＢＩＯＳに予め登録された携帯情報機器を携帯するユーザーがパソ

コンの近くにいる場合は、既に通信モジュール間で無線リンクが形成されていて認識情報の交換が行われているので、ステップＳ２ではＹｅｓと判断される。

ＢＩＯＳはこの判断を受けて、ディスプレイ画面をパスワード入力画面に遷移させ、携帯情報機器３からのパスワード入力の待機状態となる（ステップＳ３）。このとき、パソコン１の通信モジュール２と携帯情報機器３の通信モジュール４は、Ａｃｔｉｖｅモードに遷移し、携帯情報機器とパソコン間でデータ通信が行えるように成る。

なおこの時のパスワードは、ＢＩＯＳでサポートされている数字入力によるブートロックパスワードである。

ユーザーがパソコンのパスワード入力画面上の案内にしたがって、携帯情報機器３からパスワードを入力すると、ＢＩＯＳはそのパスワードが予め登録されたものであるかどうかをステップＳ４において判断し、登録されたものである場合（ステップＳ４のＹｅｓ）には、ブートシーケンスを開始して（ステップＳ５）、ＯＳを起動する（ステップＳ６）。ＯＳ起動後の通信モジュールは、ＯＳ上のブルートゥースアプレットに依存して低消費電力状態に遷移する。なお、この低電力状態でもピコネットは維持されている。

一方、ステップＳ４で入力されたパスワードが登録されたものでは無いと判断された場合は、ＢＩＯＳはステップＳ４に戻ってパスワードの再入力を要請し、入力されたパスワードが正しいか否かを再び判断する。このように、正しいパスワードが入力されるまで、ＢＩＯＳはＯＳを起動しない。

図３に本実施形態におけるＢＩＯＳセットアップセキュリティメニュー画面の一例を示す。本装置では、標準状態のセキュリティモードに対して携帯電話が設定されており、パスワードの設定は携帯

電話から行うように指示されている。

図４の（ａ）にユーザー用パスワードの新規設定時のディスプレイ画面を、図４（ｂ）にユーザー用パスワードの変更時のディスプレイ画面を示す。いずれの場合にも、画面の案内にしたがって、携帯情報機器からパスワードを入力する。なお、パソコンがネットワークに組み込まれているときは、管理者用のパスワード設定も可能であるが、そのときも同様に携帯情報機器からのパスワード入力とする事によって、セキュリティを強化する事ができる。

図５は、就業中のＢＩＯＳにおけるセキュリティチェック手順を示すフローチャートである。ＢＩＯＳは定期的にパソコン１と携帯情報機器３との通信モジュール２，４の状態を監視しており、両者の間で正常にリンクが形成されているか否かを判断している（ステップＴ１）。今、ユーザーがパソコン１を使用状態にしたまま席を離れる等して携帯情報機器３がパソコン１の通信可能範囲から離れた場合、通信リンクが切れるため通信モジュール２，４は自動的にＳｔａｎｄｂｙモードに移行する。

これによってステップＴ１ではＮｏと判断され、ＢＩＯＳはディスプレイ画面（またはステータスＬＣＤ）にパスワードロックの状態を表示し（ステップＴ２）、キーボード、マウス等の入力デバイスをロックしてその使用を禁止し（ステップＴ３）、その後省電力状態に移行する。

この結果、ユーザーが不用意に席を離れた場合であっても、正規のユーザー以外の人間による当該パソコンの不正使用が防止される。

図６は、ユーザーが席に戻って省電力状態のパソコン１のリジュームボタンを押下して、再び使用を開始する場合のＢＩＯＳのセキュリティチェック手順を示すフローチャートである。なおこの手順

は、ユーザーがサスペンドボタンを押下して、パソコン１を強制的に省電力状態に移行させた場合からの復帰手順と同じである。

ユーザーが席を離れたり、あるいはサスペンドボタンを押下してステップＲ１でパソコン１が省電力モードにある場合、ユーザーが帰席してリジュームボタンを押下する（ステップＲ２）と、ＢＩＯＳは予め登録されたＩＤを持つ携帯情報機器３が近くにあるか否かを判定し（ステップＲ３）、携帯情報機器３が近くにある場合（ステップＲ３のＹｅｓ）、パソコン１を省電力状態から復帰させ（ステップＲ４）、パスワード入力画面をディスプレイに表示する（ステップＲ５）。

この状態で、携帯情報機器３からユーザーが正しいパスワードを入力する（ステップＲ５のＹｅｓ）と、入力デバイスのロック状態を解除し、ＯＳを元の状態に復帰させる（ステップＲ６）。一方、ステップＲ３で登録された携帯情報機器が近くに無いと判断された場合（Ｎｏ）は、リジュームボタンの押下にかかわらず、入力デバイスのロック状態を維持する。

また、ステップＲ５で正確なパスワードが入力されなかった場合は、パスワードの入力画面に戻りパスワードの携帯情報機器よりの再入力を要請する。ここで、例えば３回正しいパスワードの入力に失敗すると、ステップＲ１に戻り、パソコン１を強制的に省電力状態に移行させることにより、更なるセキュリティの強化を図ることができる。

なお、上記の実施形態では、セキュリティをさらに強化するためにパスワードの入力は携帯情報機器３から行う構成とされているが、あるいは、パソコンのキーボードより行う構成であってもよい。さらに、携帯情報機器３からのパスワード入力の場合、音声によるパスワード入力とする事も可能である。この場合には、音声情報の

テキスト情報への変換ソフトが必要である。

図７は、図１に示すパソコン１の概略構成を示すブロック図である。１１はパソコンを構成する各部の動作を制御するためのシステムコントローラ、１２はＣＰＵ、１３はＤＲＡＭ等で構成される主記憶装置である。さらにこの装置には、外部記憶装置としてハードディスク１４、ＣＭＯＳ・ＲＡＭ１５、ディスプレイ１６、キーボード１７、マウス１８等が接続されており、それぞれディスクコントローラ１９、ディスプレイコントローラ２０、キーボードコントローラ２１によって制御されている。

本装置には更にＢＩＯＳを格納するためのフラッシュメモリ２２、ＵＳＢコントローラ２４が設けられ、Ｉ／Ｏコントローラ２３はシリアルポート２５、パラレルポート２６、フロッピディスクドライブ２７等を制御し、ＵＳＢコントローラ２４は、ＵＳＢ端子を介して接続された例えばデジタルカメラ２８、あるいはプリンタ（図示せず）を制御する。なお、図７において２９はＣＭＯＳ・ＲＡＭ５を駆動するためのバッテリ、２０は外部の例えば商用電源から本装置を駆動するための電力を得るための電源部を示す。

なお、上記構成はあくまでも１例であってその構成に限定されるものではなく、さらに各部の構成及びその動作は周知であるのでここで特別に説明しない。

本発明の１実施形態では、上記のように構成されたパソコンにＵＳＢコントローラ２４を介してブルートゥース対応の通信モジュール３１が接続されている。なお、通信モジュール３１はＵＳＢ対応の外付け装置として構成されるのみならず、図に点線で示すように（３１’）システムコントローラ１に直接接続しても良い。いずれの構成を採用するかは、パソコンの設計にあたって任意に選択できる。

なお、通信モジュール３１（３１’）は１チップのＣＭＯＳＬＳＩとアンテナで構成される。

上述した本発明の実施形態は、パソコン１に対して携帯情報機器３を１対１で対応付けるものであるが、ＢＩＯＳにおける事前の登録によって、パソコンが複数の携帯情報機器を認識しそれぞれにパスワードを割り付けることが可能である。これは通常ブルートゥースモジュールが同時に複数の機器をピコネットで接続することができるためである。このようにする事によって、１台のパソコンを複数のユーザーによって高いセキュリティを維持しながら共用する事ができる。

発明の効果

以上の様に、本発明の情報処理装置のセキュリティシステムでは、あらかじめＢＩＯＳに登録された通信モジュールを有する携帯情報機器を身に付けた、あるいはそばに置いたユーザーがパソコン等の情報処理装置の近傍にいない限り情報処理装置の電源がオンと成った場合でも、ディスプレイ画面はパスワード入力画面に移行しない。従って携帯情報機器が他人に盗用された場合でも、パスワードを入力しない限りＯＳが起動されないので、一段のセキュリティ強化を図る事ができる。

携帯情報機器としては、汎用の携帯電話、ＰＤＡなど既存のシステムを応用できるので、セキュリティシステムとして特別なハードウエアの構築を必要とせず、容易にかつ安価に実現する事が可能である。

またさらに、ＢＩＯＳに予め登録されたパスワードをその携帯情報機器から入力しない限りＯＳが起動されない設定とすることによって、さらにセキュリティ機能を強化することができる。

一方、パスワードを入力した状態でパソコン等の情報処理装置からユーザーが離れた場合には、モジュール間の通信リンクが切れるため、この状態を利用して入力デバイスの使用禁止状態を設定する構成としている。その結果、パスワード入力済みの状態でも他人の不正利用に対するセキュリティを強化することができる。

請　求　の　範　囲

１．無線によるデータ通信が可能な第１の通信モジュールを備えた情報処理装置と、前記第１の通信モジュールと無線通信リンクを形成可能な第２の通信モジュールを備えた携帯情報機器とを備え、前記情報処理装置は、前記第１および前記第２の通信モジュール間で通信リンクが形成された場合のみパスワード入力画面に移行するように設定されている、情報処理装置のセキュリティシステム。

２．前記情報処理装置は前記携帯情報機器から予め登録されたパスワードの入力を受信した場合のみＯＳを起動するものである、請求項１に記載の情報処理装置のセキュリティシステム。

３．前記第１、第２の通信モジュールはブルートゥース対応の通信モジュールである、請求項１または２に記載の情報処理装置のセキュリティシステム。

４．前記情報処理装置はＯＳの起動中において、前記第１および第２の通信モジュール間で通信リンクが切れたことを認識して入力デバイスをロック状態に移行させるものである、請求項１乃至３の何れか１項に記載の情報処理装置のセキュリティシステム。

５．前記入力デバイスはキーボードおよびマウスである、請求項４に記載の情報処理装置のセキュリティシステム。

６．前記情報処理装置は、リジュームボタンが操作されると、前記第１と第２の通信モジュール間で通信リンクが確立されている場合のみパスワード入力画面に移行し、予め登録されたパスワードの入力によってＯＳを復帰させる、請求項５に記載の情報処理装置のセキュリティシステム。

７．前記携帯情報機器を複数個備え、前記第１の通信モジュールは前記複数の携帯情報機器の第２の通信モジュールのそれぞれを認

識可能である、請求項１に記載の情報処理装置のセキュリティシステム。

８．前記情報処理装置は、前記複数の携帯情報機器のそれぞれの第２の通信モジュールに対してそれぞれ異なるパスワードを割り付けている、請求項７に記載の情報処理装置のセキュリティシステム。

９．前記携帯情報機器は携帯電話である、請求項１乃至８の何れか１項に記載の情報処理装置のセキュリティシステム。

１０．前記携帯情報機器はＰＤＡである請求項１乃至８の何れか１項に記載の情報処理装置のセキュリティシステム。

１１．前記パスワードは前記携帯情報機器を介して音声にて入力可能である請求項２に記載の情報処理装置のセキュリティシステム。

１２．無線によるデータ通信が可能な通信モジュールを備え、該通信モジュールが外部無線通信モジュールと通信リンクを形成する場合にパスワード入力画面に移行するように設定された情報処理装置。

Fig.1

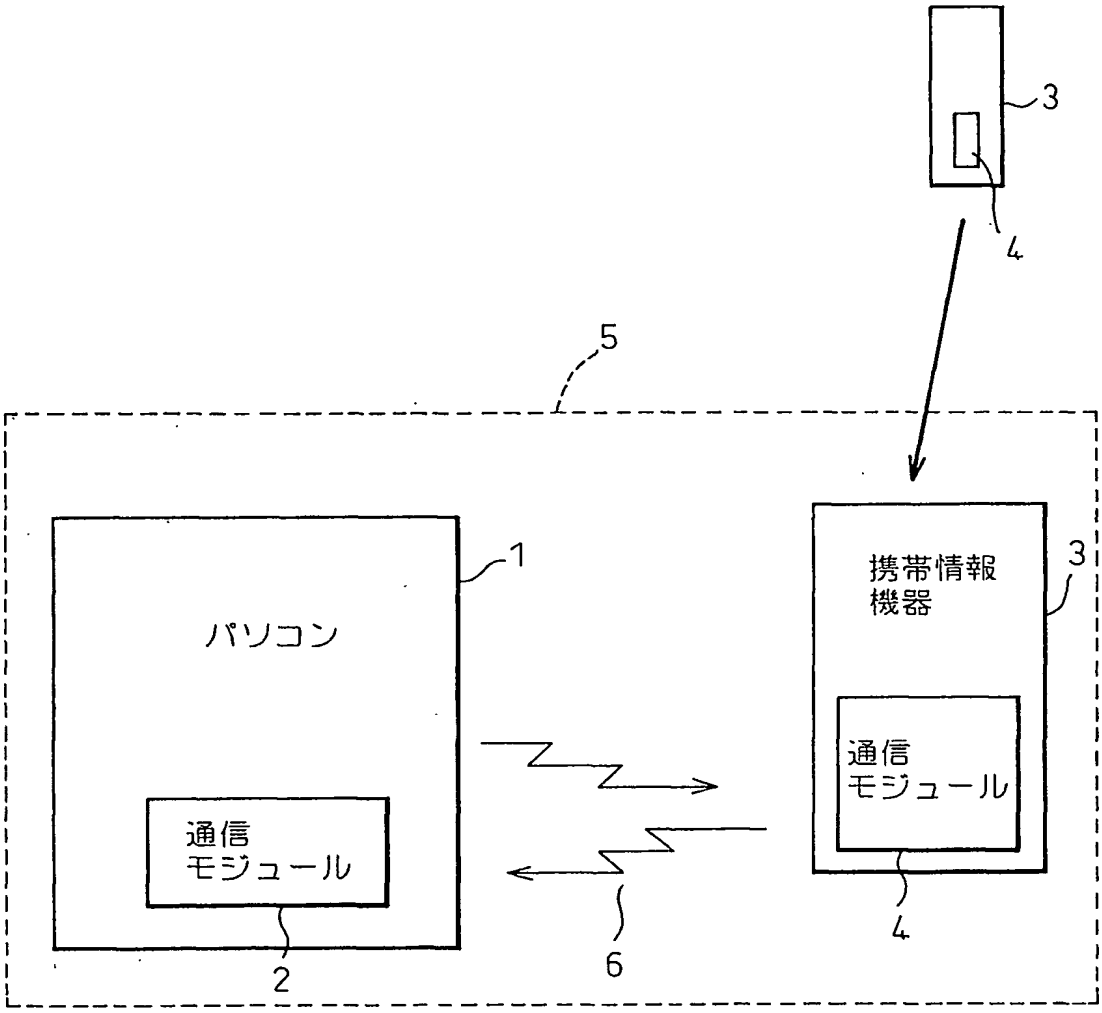


Fig.2

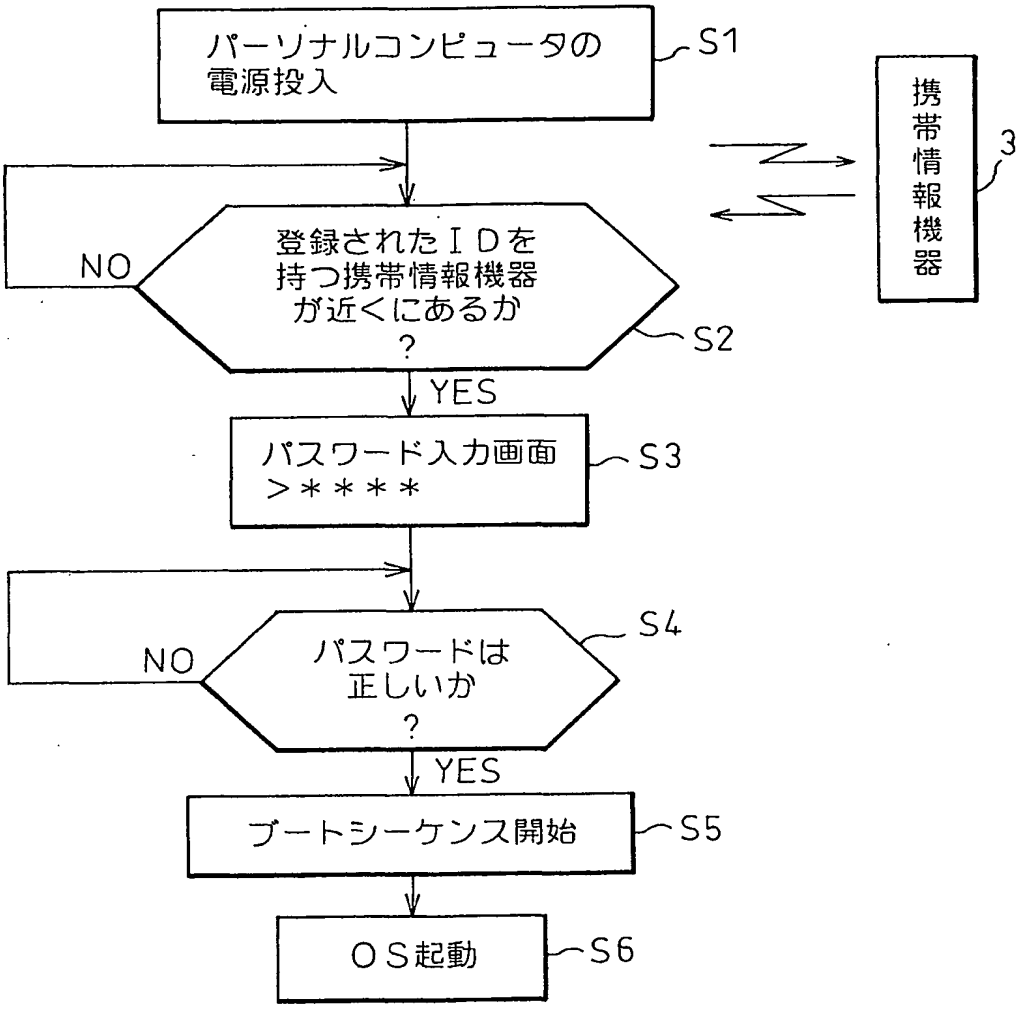

パーソナルコンピュータの
電源投入
S1
携帯情報機器
3
NO
登録されたＩＤを
持つ携帯情報機器
が近くにあるか
？
S2
YES
パスワード入力画面
＞＊＊＊＊＊
S3
NO
パスワードは
正しいか
？
S4
YES
ブートシーケンス開始
S5
ＯＳ起動
S6

Fig.3

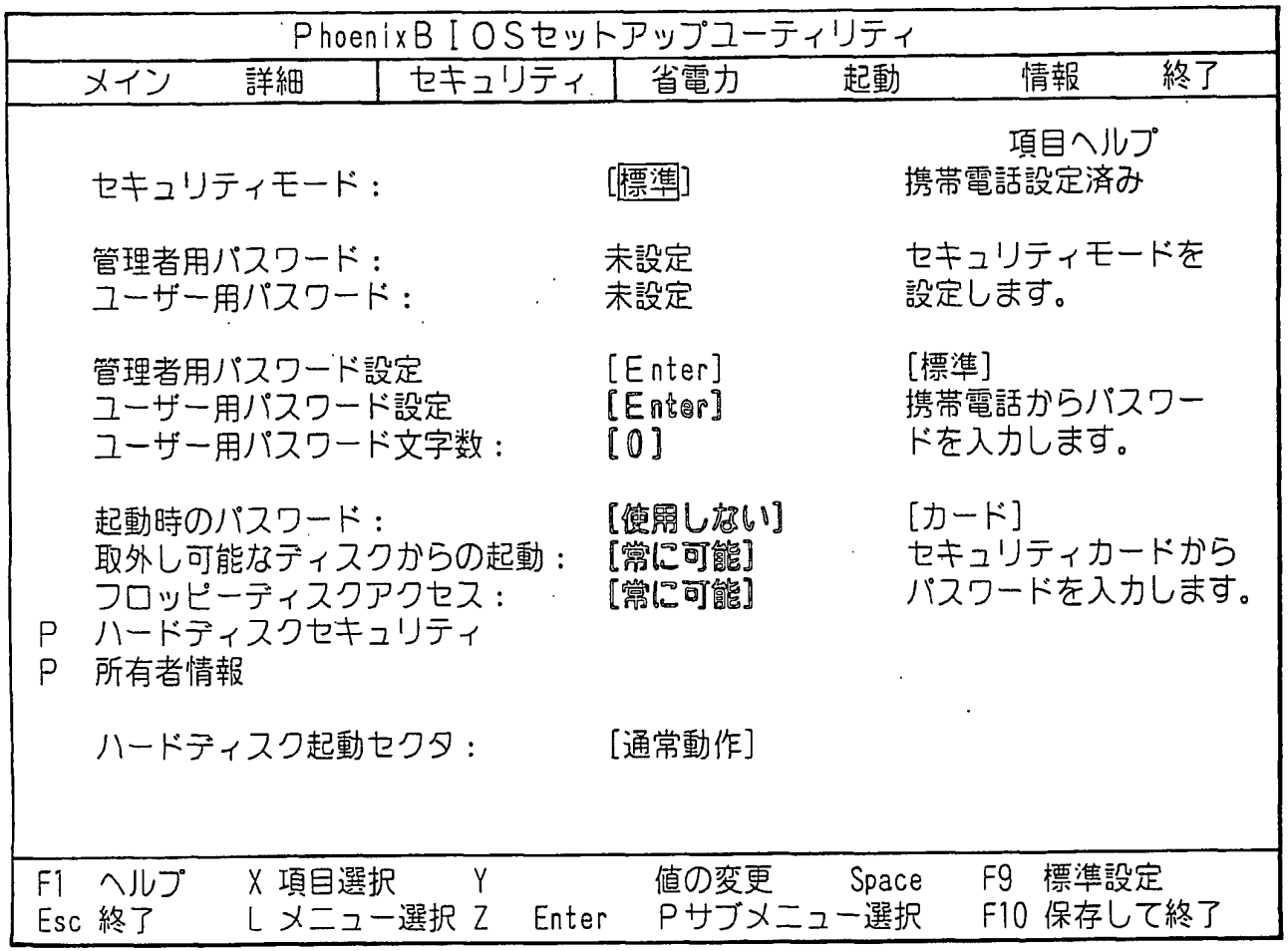

PhoenixBIOSセットアップユーティリティ
メイン
詳細
セキュリティ
省電力
起動
情報
終了
項目ヘルプ
セキュリティモード：
[標準]
携帯電話設定済み
管理者用パスワード：
未設定
ユーザー用パスワード：
未設定
セキュリティモードを
設定します。
管理者用パスワード設定
[Enter]
ユーザー用パスワード設定
[Enter]
ユーザー用パスワード文字数：
[0]
[標準]
携帯電話からパスワー
ドを入力します。
起動時のパスワード：
[使用しない]
取外し可能なディスクからの起動：
[常に可能]
フロッピーディスクアクセス：
[常に可能]
[カード]
セキュリティカードから
パスワードを入力します。
P ハードディスクセキュリティ
P 所有者情報
ハードディスク起動セクタ：
[通常動作]
F1 ヘルプ
X 項目選択
Y
値の変更
Space
F9 標準設定
Esc 終了
L メニュー選択 Z
Enter
Pサブメニュー選択
F10 保存して終了

Fig.4(a)

ユーザー用パスワードの設定

新しいパスワードを携帯電話から入力して下さい。 [V]
新しいパスワードを確認して下さい。 [ ]

Fig.4(b)

ユーザー用パスワード設定

現在のパスワードを携帯電話から入力して下さい。 [V]
新しいパスワードを携帯電話から入力して下さい。 [ ]
新しいパスワードを確認して下さい。 [ ]

Fig.5

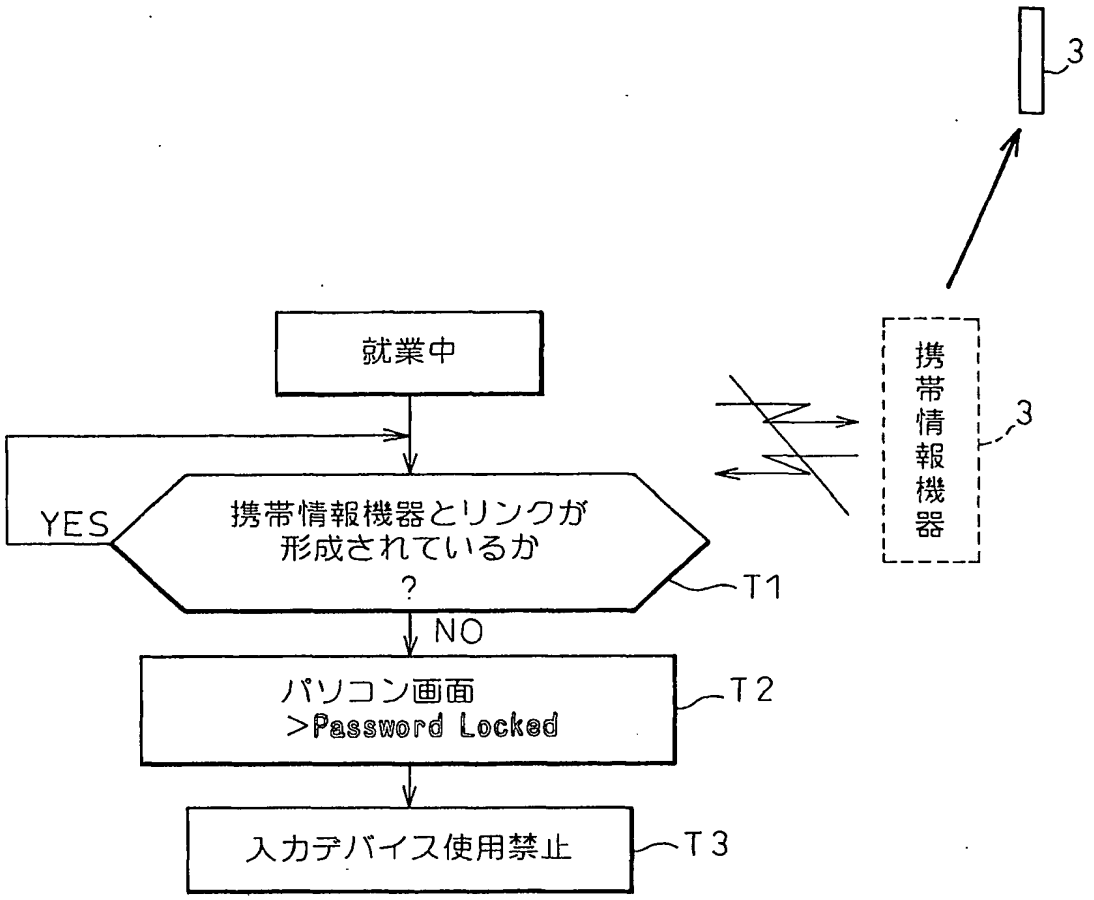

3
就業中
携帯情報機器
3
YES
携帯情報機器とリンクが
形成されているか
?
T1
NO
パソコン画面
>Password Locked
T2
入力デバイス使用禁止
T3

Fig.6

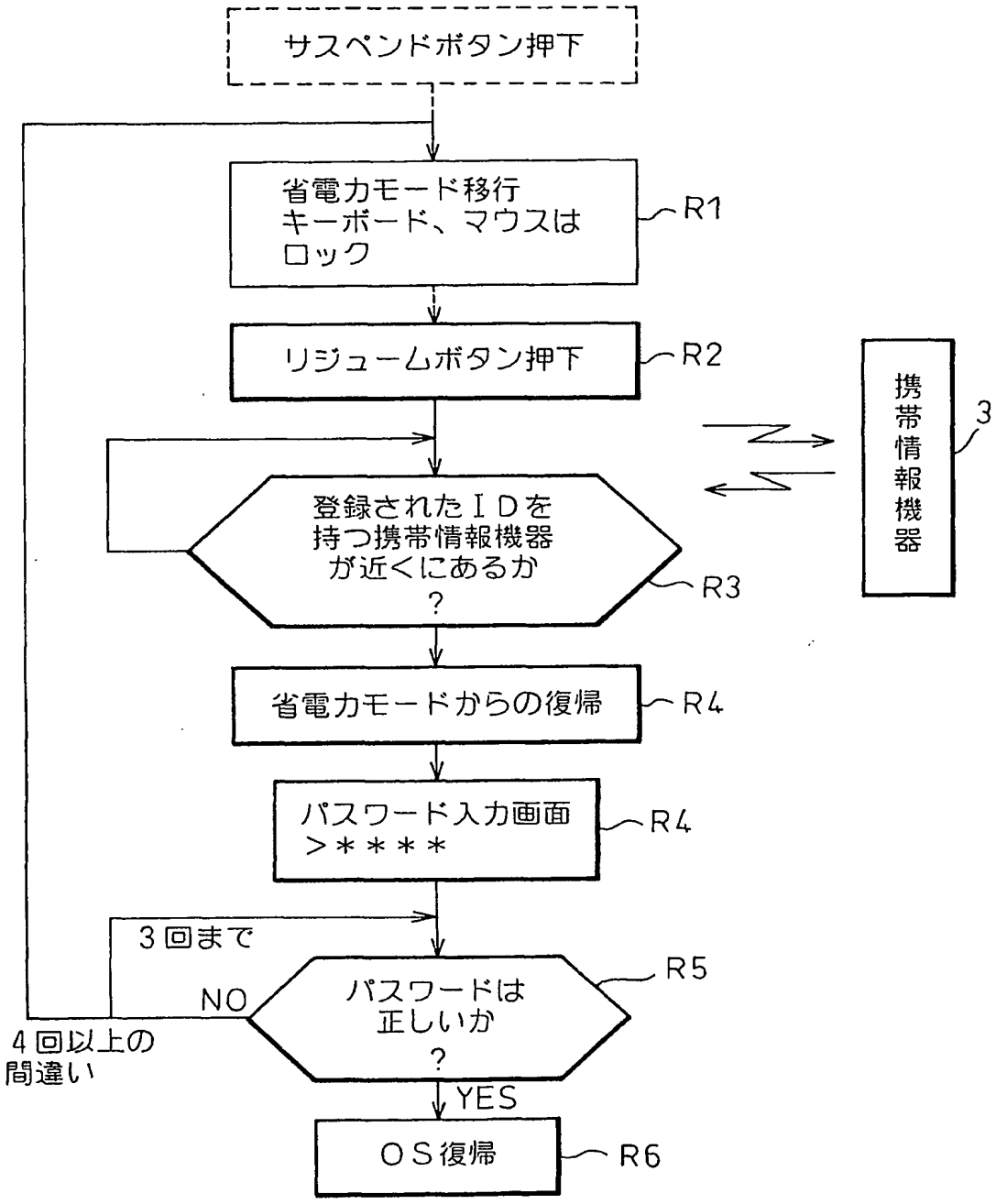
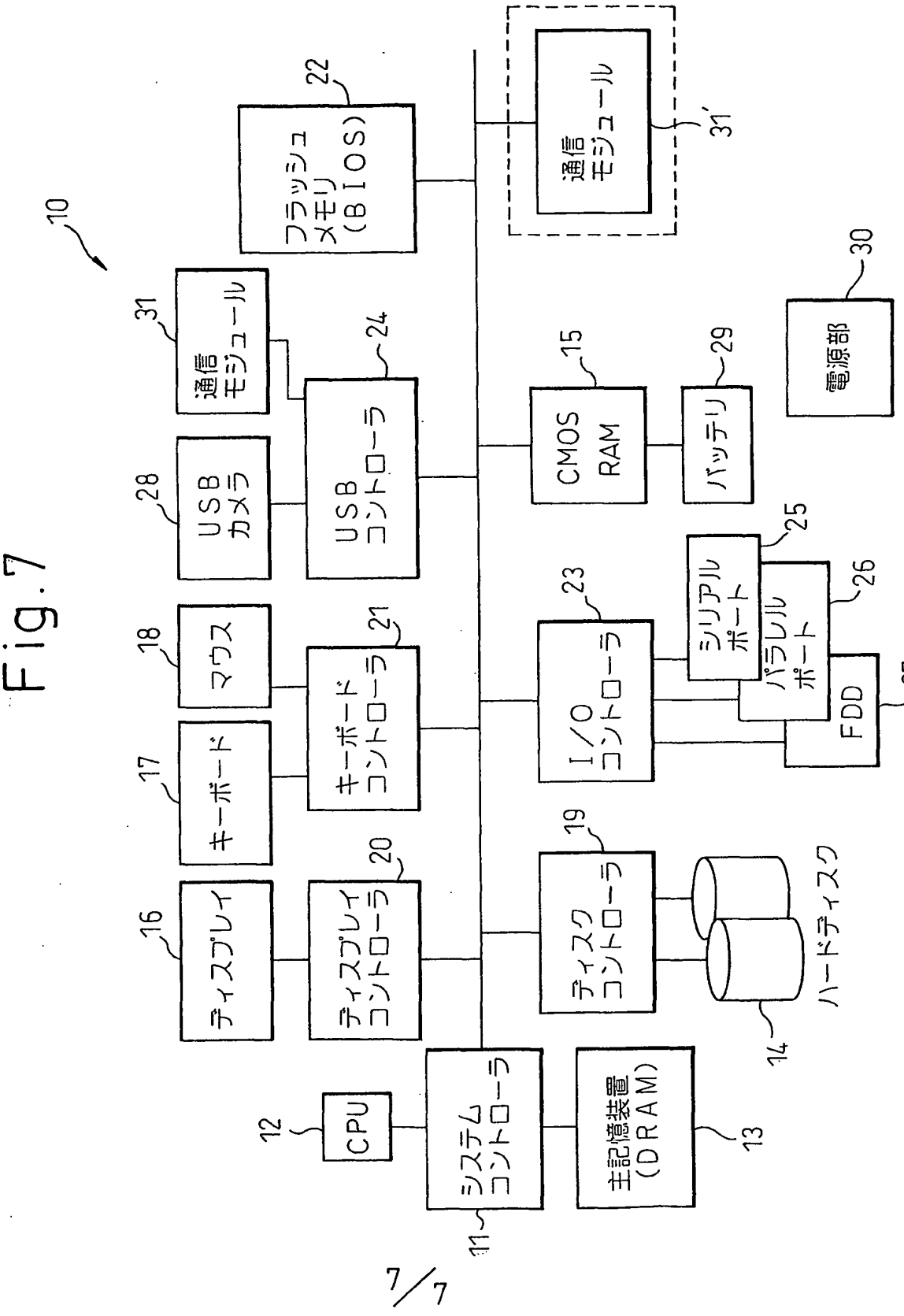

サスペンドボタン押下
省電力モード移行
キーボード、マウスは
ロック
R1
リジュームボタン押下
R2
携帯情報機器
3
登録されたＩＤを
持つ携帯情報機器
が近くにあるか
？
R3
省電力モードからの復帰
R4
パスワード入力画面
＞＊＊＊＊
R4
3回まで
NO
パスワードは
正しいか
？
R5
4回以上の
間違い
YES
ＯＳ復帰
R6

Fig. 7


10
CPU
12
システム
コントローラ
11
主記憶装置
(DRAM)
13
ハードディスク
14
ディスク
コントローラ
19
ディスプレイ
コントローラ
20
ディスプレイ
16
キーボード
コントローラ
21
キーボード
17
マウス
18
USB
コントローラ
24
USB
カメラ
28
通信
モジュール
31
フラッシュ
メモリ
(BIOS)
22
通信
モジュール
31'
I/O
コントローラ
23
CMOS
RAM
15
バッテリ
29
電源部
30
シリアル
ポート
25
パラレル
ポート
26
FDD
27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/08256

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F1/00, G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F1/00, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 10-149339 A (Mitsubishi Electric Corporation), 02 June, 1998 (02.06.1998), Par. Nos. [0003] to [0006] (Family: none)	1,2,4-6,11,12 3,7-10
Y	JP 11-288402 A (Yazaki Corporation), 19 October, 1999 (19.10.1999), Par. No. [0044] (Family: none)	3,7-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 December, 2000 (12.12.00)	26 December, 2000 (26.12.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP00／08256

A.　発明の属する分野の分類（国際特許分類（IPC））

Int Cl' G06F1／00, G06F15／00, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int Cl' G06F1／00, G06F15／00、H04L9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2000年
日本国登録実用新案公報　1994－2000年
日本国実用新案登録公報　1996－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP，10－149339，A（三菱電機株式会社）2．6月．1998（02．06．98），段落【0003】～【0006】（ファミリなし）	1,2,4-6,11,12 3，7－10
Y	JP，11－288402，A（矢崎総業株式会社）19．10月．1999（19．10．99），段落【0044】（ファミリなし）	3，7－10

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
12．12．00	26.12.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	田中　貞嗣 印	5E　9741
	電話番号　03－3581－1101　内線　3520	

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference H817-PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP00/08256	International filing date (*day/month/year*) 22 November 2000 (22.11.00)	Priority date (*day/month/year*)
International Patent Classification (IPC) or national classification and IPC G06F 1/00, 15/00, H04L 9/32		
Applicant FUJITSU LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 28 March 2001 (28.03.01)	Date of completion of this report 28 September 2001 (28.09.2001)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP00/08256

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP00/08256

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-12	NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

Document 1: JP, 2000-276247, A (Mitsubishi Electric Corp.), 6 October, 2000 (06.10.00), paragraphs [0034]-[0040] (Family: none)
Document 2: JP, 10-149339, A (Mitsubishi Electric Corp.), 2 June, 1998 (02.06.98), paragraphs [0023]-[0031] and [0142]-[0143] (Family: none)
Document 3: JP, 2000-224156, A (International Business Machines Corp.), 11 August, 2000 (11.08.00), paragraphs [0009] and [0032]-[0039] (Family: none)
Document 4: JP, 2000-222059, A (Sharp Corp.), 11 August, 2000 (11.08.00), paragraphs [0011]-[0019] (Family: none)

The subject matters of claims 1, 2, 7, 8, 11 and 12 do not appear to involve an inventive step in view of document 1, and document 2 cited in the ISR. The terminal security system described in document 1 and the information processing method described in document 2 belong to technical fields closely related to each other. So, a person skilled in the art could have easily conceived of applying the password input in a portable security input device described in document 2 to the startup of a terminal described in document 1.

The subject matters of claims 3, 9 and 10 do not appear to involve an inventive step in view of documents 1-3. The terminal security system described in document 1 and the authentication by means of Bluetooth described in document 3 belong to technical fields closely related to each other. So, a person skilled in the art could have easily conceived of applying the authentication by means of Bluetooth described in document 3 to the radio communication described in document 1.

The subject matters of claims 4-6 do not appear to involve an inventive step in view of documents 1-4. The terminal security system described in claim 1 and the fraudulence preventive means for an information processor described in document 4 belong to technical fields closely related to each other. So, a person skilled in the art could have easily conceived of applying the input permission inhibitory control means described in document 4 to the non-authentication for a busy terminal described in document 1.